

明 細 書

暗号方式の安全性を保証するパディング適用方法

化装置

技術分野

- [0001] 本発明は情報の暗号化／復号化システムに係り、特に選択暗号文攻撃に対し安全性を保証するパディング適用方法および暗号化／復号化装置に関する。

背景技術

- [0002] 通信のセキュリティを確保するために暗号技術の社会的応用が盛んに進められ、効率的な暗号計算が従来以上に望まれている。このような傾向のなかで、Jeffrey Hoffstein、Jill PipherおよびJoseph H. Silvermanによる文献“NTRU: A Ring-Based Public Key Cryptosystem” (非特許文献1) により提案されたNTRU暗号方式は、従来のRSA暗号方式やElGamal暗号方式と比べ、メモリ消費が少なく高速な暗号／復号計算方法として注目されている。
- [0003] (NTRU暗号化方式)
- NTRU暗号方式は以下のような公開鍵暗号方式である。
- [0004] まず以下のようにして鍵生成を行う。正整数 p , q , N をとり領域変数として公開し、 $R = \mathbb{Z}[X]/(X^N - 1)$ とする。以下、 $L(a, b)$ は、 R の元 u であって、 u の各次数の係数のうち a 個が1で b 個が-1、他のものが0であるもの全体の集合 (R の部分集合)を表すものとする。パラメータ df , dg , d を決め、 $L_f = L(df, df+1)$, $L_g = L(dg, dg+1)$, $L_\phi = L(d, d)$ とする。 L_f から f を、 L_g から g をランダムに取り、 $h = f^{-1}g \bmod q$ とする。 f , g を秘密鍵とし、 h を公開鍵とする。
- [0005] 鍵が生成されると、 R の部分集合 L_m の元 m を暗号化する。まず、 R の部分集合元 L_r から r をランダムに選び、 $e = phr + m \bmod q$ を計算し、 e を暗号文として出力する。
- [0006] 暗号文 e から元の平文 m を復号するには、まず $fe = pgr + fm \bmod q$ を計算する。 f , g , r , m がそれぞれ L_f , L_g , L_r , L_m の元であることから $fe = pgr + fm$ であるので、 $fe \bmod p = m \bmod p$ を計算することができ、 m が L_m の元であることから $m = m \bmod p$ なので m を復元できる。

- [0007] しかしながら、Don Coppersmith、Adi Shamirによる文献“Lattice Attacks on NTRU”
 , Eurocrypt'97 Springer Lecture Notes in Computer Sciences,1997(非特許文献2)
 などに指摘されているように、NTRU暗号方式には数々の解読方法が知られている。
 これに対して、平文に何らかのパディングを施した後、NTRU暗号化することにより解
 読を防御する方法が幾つか知られている。
- [0008] (OAEP+パディング方式)
 暗号方式を安全にするためのパディング方法としては、例えばVictor Shoupによる
 文献“OAEP Reconsidered”Journal of Cryptology 15(4)(非特許文献3)で提案された
 OAEP+と呼ばれるパディング方法が知られている。OAEP+パディングは以下のような
 パディング方式である。
- [0009] まず、パラメータ k, k_0, k_1 を次のように選ぶ: k, k_0, k_1 は正整数、かつ、 $k_0 + k_1 \leq k \leq L$ を満たす。ここで、 L は平文空間の元の数である。
- [0010] さらに、 $n = k - k_0 - k_1$ とし、
 G は、 k ビットのビット列に n ビットのビット列を対応させるハッシュ関数、
 H' は、 $n+k_0$ ビットのビット列に k_1 ビットのビット列を対応させるハッシュ関数、および、
 H は、 $n+k_1$ ビットのビット列に k_0 ビットのビット列を対応させるハッシュ関数とする。
- [0011] パディング装置は n ビットの平文 M を受け取り、 k_0 ビットのビット列 R をランダムに選ぶ。
 続いて、 $G(R)$ と M のビット毎の排他的論理和 s^0 を計算し、 $s^1 = H'(R||M)$ を計算し、 $s = s^0 || s^1$ とする。ここで「 $||$ 」はビット列の接続を表す。 t を $H(s)$ と R のビット毎の排他的論理和とし、 $w = s || t$ とする。この w を「平文 M の乱数 R を用いたOAEP+パディング」と呼ぶ。こうして得られたOAEP+パディング w を(乱数を使わない暗号方式で)暗号化し、暗号文 e を受信者に送信する。
- [0012] 受信者は、受信した暗号文 e を復号し、 w を得る。 w を復号後、パディング復元装置は以下のようにして平文 M を復元する。まず w は $w = s || t = s_0 || s_1 || t$ の形をしているので、これを使って s_0, s_1, t を復元する。次に $H(s)$ と t のビット毎の排他的論理和を取ることで R を復元する。 $G(R)$ と s_0 のビット毎の排他的論理和を計算することにより M を復元する。 $s_1 = H'(R||M)$ を満たせば M を出力し、満たさなければ e は不正な暗号文として「 \perp 」を出力する。

- [0013] しかしながら、このOAEP+パディングは、暗号化関数を計算する際に乱数を使用しない暗号方式に対して適応するために提案されたパディング方式である。このために、上述したNTRUのような乱数を使用した暗号方式に適応した場合は必ずしも安全性が保証されないという問題がある。また、NTRUのような乱数を使用した暗号方式にOAEP+パディングを適応する場合には、適応方法は一意ではなく様々な方法を考えることができるために、どのようなパディングの適用方法が安全で、どのようなパディングの適用方法が安全でないかがすぐには分からないという問題もある。
- [0014] このようにOAEP+パディング方式は乱数を使用しない暗号方式に対してのみ安全性が保証できるのであるが、乱数を使用するNTRU暗号方式に対してOAEP+パディング方式ないしそれに類似したパディング方式を適応することで安全性を保証しようという試みもいくつか提案されている。たとえば、次の文献を参照されたい。
- [0015] ・Joseph H. Silvermanによる文献“Plaintext Awareness and the NTRU PKCS”
Technical Report#7 version 2, NTRU Cryptosystems, 1998(非特許文献4)
・Jeffrey Hoffstein、Joseph H. Silvermanによる文献“Optimizations for NTRU”
Public-key Cryptography and Computational Number Theory(非特許文献5)
・Jeffrey Hoffstein、Joseph H. Silvermanによる文献“Protecting NTRU Against
Chosen Ciphertext and Reaction Attacks”Technical Report, NTRU Cryptosystems,
2000, Report#16 version 1(非特許文献6)
・Phong Q. Nguyen、David Pointchevalによる文献“Analysis and Improvements of
NTRU Encryption Paddings”Crypto 2002 Springer Lecture Notes in Computer
Sciences, 2002(非特許文献7)。
- [0016] しかしながら、これらのパディングつきNTRU暗号方式はすべて解読された。非特許文献4に記載されたパディングを施したNTRU暗号方式は、Eliane Jaulmes、Antoine Jouxによる文献“A Chosen-Ciphertext Attack against NTRU”Crypto 2000 Springer Lecture Notes in Computer Sciences, 2000(非特許文献8)で提案されたアルゴリズムで解読された。
- [0017] また、非特許文献5および6に記載されたパディングを施したNTRU暗号方式は非特許文献7で提案されたアルゴリズムで解読され、この非特許文献7によるパディング

方法はJohn A. Proosによる“Imperfect Decryption and an Attack on the NTRU Encryption Scheme”(非特許文献9)により解読された。

- [0018] OAEP+パディング方式以外のパディング方式を用いてNTRU暗号方式のような乱数を使った暗号方式の安全性確保を図った方式も提案されているが、パディング方式は方式毎に異なる弱点を持っているために、OAEP+パディングを用いて暗号方式の安全性を確保することは依然として有意義である。

非特許文献1:Jeffrey Hoffstein、Jill PipherおよびJoseph H. Silvermanによる文献“NTRU:A Ring-Based Public Key Cryptosystem”

非特許文献2:“Lattice Attacks on NTRU”, Eurocrypt'97 Springer Lecture Notes in Computer Sciences,1997

非特許文献3:“OAEP Reconsidered”Journal of Cryptology 15(4)

非特許文献4:“Plaintext Awareness and the NTRU PKCS” Technical Report#7 version 2, NTRU Cryptosystems, 1998

非特許文献5:Jeffrey Hoffstein、Joseph H. Silvermanによる文献“Optimizations for NTRU” Public-key Cryptography and Computational Number Theory

非特許文献6:“Protecting NTRU Against Chosen Ciphertext and Reaction Attacks” Technical Report, NTRU Cryptosystems, 2000, Report#16 version 1

非特許文献7:“Analysis and Improvements of NTRU Encryption Paddings”Crypto 2002 Springer Lecture Notes in Computer Sciences, 2002

非特許文献8:“A Chosen-Ciphertext Attack against NTRU”Crypto 2000 Springer Lecture Notes in Computer Sciences, 2000

非特許文献9:John A. Proosによる“Imperfect Decryption and an Attack on the NTRU Encryption Scheme”

発明の開示

発明が解決しようとする課題

- [0019] 上述したように、従来のパディングつきNTRU暗号方式は安全な暗号通信を行うことができない。

- [0020] 本発明の目的はNTRU暗号方式のような方式に対して適切なパディングを施すこと

で安全な暗号通信を達成するパディング適用方法および暗号化／復号化装置を提供することにある。

課題を解決するための手段

- [0021] 本発明者は、NTRU暗号方式では暗号に使用した乱数を復元可能であることに着目し、暗号通信の安全性を保証できる新規なパディング適用方式を発明した。
- [0022] (成立根拠)
- まず、本発明の成立根拠について簡単に説明する。乱数を使用した暗号方式で代表的なものに、エルガマル暗号方式やペイリエー暗号方式などがある。これらの暗号方式では、暗号文受信者が平文を復元することはできるが乱数を復元することはできないために、平文と乱数とは全く異なる種類のデータとして扱う必要がある。
- [0023] また、エルガマル暗号方式やペイリエー暗号方式等の多くの暗号方式では、暗号化関数は確率的な関数であり、暗号化関数の定義域は平文M全体の空間であり、値域は暗号文全体の空間である。それに対し、復号化関数は確率を使わない関数であり、定義域は暗号文全体の空間で値域は平文全体の空間である。繰り返すが、これらの暗号方式では暗号に使用した乱数を復元できない。
- [0024] これに対して、NTRU暗号方式は、平文 m を復元した後に、 $r = (fe - fm)/pg$ により乱数 r を求めることができる、という特徴がある。このため、NTRU暗号方式は、エルガマル暗号方式やペイリエー暗号方式等の暗号方式とは異なり、平文と乱数とを区別する必然性がない。
- [0025] したがって、NTRU暗号方式では、次のようにみなすことができる。
- [0026] ・暗号化関数は乱数を使わない関数であり、その定義域は平文Mと乱数Rとの接続全体の空間、値域は暗号文全体の空間である。
- [0027] ・復号化関数も乱数を使わない関数であり、その定義域は暗号文全体の空間、値域は平文Mと乱数Rとの接続全体の空間である。
- [0028] 既に述べたようにOAEP+パディングは暗号化関数が乱数を使わない場合には安全性が保証される。したがって、NTRU暗号方式の平文と乱数とを区別しないデータ構造に対して、安全性保証つきOAEP+パディングを適用可能であることがわかる。
- [0029] (本発明の概要)

この知見に基づいて、本発明がなされた。すなわち、本発明によるパディング適用方式は、暗号文作成者が暗号文の作成に使用した乱数の値を暗号文受信者が復元できる暗号方式 $E'(m)$ に対して適用可能であり、このような暗号方式に対して本発明を適用した場合に安全性が保証される。

- [0030] 本発明によれば、暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用する方法は、入力情報を前記パディング方式により所定長以下のビット列に変換し、前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換し、前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給し、前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、ことを特徴とする。
- [0031] 本発明の一実施形態によれば、変換規則は、前記ビット列の前半を前記第1ビット列とし、後半を前記第2ビット列とするように前記ビット列を2分割する規則である。
- [0032] 本発明の一実施例によれば前記パディング方式はOAEP+パディングであり、前記乱数を使用する暗号化方式はNTRU暗号方式である。
- [0033] 図1(A)は、本発明によるパディング適用方式による暗号化装置の概念的ブロック図であり、(B)は従来例によるOAEPベースのパディング方式を適用した暗号化装置の概念的ブロック図である。ただし、パラメータは最も標準的な場合が示されており、 $n = k_0 = k_1$ であり、 m のビット数は r である。
- [0034] 図1(A)を用いて本発明によるパディング適用方式を説明すると、おおよそ次のようになる。まず、OAEP+パディング方式と同様のパラメータを選ぶ。すなわち、上述したように、正整数 k, k_0, k_1 を $k_0 + k_1 < k < L$ を満たすように取る。ここで L は平文空間の元の数である。 $n = k - k_0 - k_1$ とし、 G を k ビットのビット列に n ビットのビット列を対応させるハッシュ関数、 H' を $n+k_0$ ビットのビット列に k_1 ビットのビット列を対応させるハッシュ関数、 H を $n+k_1$ ビットのビット列に k_0 ビットのビット列を対応させるハッシュ関数とする。

- [0035] 次に、 n ビットの平文 M を受け取り、OAEP+パディングを行う。すなわち k_0 ビットのビット列 R をランダムに選び、 $G(R)$ と M のビット毎の排他的論理和 s_0 を計算し、 $s_1 = H'(R||M)$ を計算して、 $s = s_0 || s_1$ とする。記号 $||$ はビット列の接続を表す。 $t = H(s)$ と R のビット毎の排他的論理和とし、 $w = s || t$ とする。
- [0036] 次に、 w を次の条件を満たす規則 A (以下、変換関数 A という。)を用いて2つのビット列 m および r を生成する。 A は、 k ビット以下のビット列に $L_m \times L_r$ の元を対応させる写像であり、ここで L_m は m の取りうる範囲、 L_r は r の取りうる範囲である。変換関数 A が満たすべき条件は次の通りである。
- [0037] (1) A は単射であること
 (2) A およびその逆写像は多項式時間で計算できること
 (3) 暗号化関数を $E(m, r)$ とした時、写像 $E: A(X) \rightarrow L_r$ は、一方向性関数であること(ただし X は (m, r) の取りうる範囲を表し、 L_r は暗号文全体の空間を表す)。
- [0038] NTRU暗号方式の場合、例えばビット列 w を前半のビット列と後半のビット列に等分割して、それぞれを m および r とすればよい。こうして2つのビット列に変換されると、 $e = E'(m)$ を計算して暗号化し、 e を暗号文受信者に送信する。
- [0039] 受信者は e を受信したら、 e を復号して m を得る。上述したように $E'(m)$ の特徴により r は復元可能であるから、 r を復元する。そして、 $w = m || r$ により w を復元する。 w を復号後、OAEP+パディングの復元と同様に M を復元する。具体的には、まず、 w は $w = s || t = s_0 || s_1 || t$ の形をしているので、これを使って s_0 、 s_1 、 t を復元する。次に、 $H(s)$ と t のビット毎の排他的論理和を取ることににより R を復元し、 $G(R)$ と s_0 のビット毎の排他的論理和を計算することにより M を復元する。 $s_1 = H'(R||M)$ を満たせば、 M を出力し、そうでなければ e は不正な暗号文として \perp を出力する。

発明の効果

- [0040] 次に、本発明による方式と従来の方式とを比較して、本発明の効果を説明する。図1(B)に一例を示すように、上述した非特許文献4〜7で提案された方式では、平文 M からOAEP+(あるいはその他の)パディング方式を使って m のみを作り上げ、 r は何らかの別の手段を用いて作っている。これらの方式は、エルガマル暗号方式やペリエー暗号方式のような受信側で平文だけが復元でき乱数は復元できない暗号方式に

対しても利用できるが、ad-hocな方法であるため安全性が保証できず、特にNTRUの場合には完全解読が可能である。

[0041] これに対して、本発明による方式は、NTRUのような暗号文受信者が平文および乱数を共に復元できる暗号方式に適用されるパディング方式である。上記の従来の方式とは異なり、平文MからOAEP+パディング方式および所定の変換規則(関数A)を使ってmおよびrの両方を作り上げる。また、従来の方式とは異なり、NTRUのような暗号文受信者が平文および乱数とともに復元できる暗号方式に対して適用した場合に安全性が保証できる。

[0042] すなわち、本発明により、NTRU暗号方式という必要メモリ量の少なくかつ暗号化復号化計算が高速な暗号方式を利用して安全な暗号通信を行うことが可能になる。

発明を実施するための最良の形態

[0043] 図2は、本発明による暗号化／復号化装置を実装した暗号通信システムの一例を示すブロック図である。ここではネットワークを通して通信端末間で暗号通信が行われる。

[0044] 送信側の通信端末は、プログラム制御プロセッサ10、乱数生成器11、プログラムメモリ12、メモリ13および送受信部14を有し、後述するように、プログラムメモリ12に格納されたOAEP+変換、変換関数Aによる変換、NTRU暗号化などの必要なプログラムを実行することで平文を暗号化し、暗号文を送受信部14からネットワークを通して宛先の受信端末へ送信する。なお、メモリ13には、公開情報や秘密鍵などの暗号化に必要な情報が格納されている。

[0045] 受信端末も同様に、プログラム制御プロセッサ20、乱数生成器21、プログラムメモリ22、メモリ23および送受信部24を有し、後述するように、プログラムメモリ22、メモリ23および送受信部24を有し、後述するように、プログラムメモリ22に格納されたNTRU復号化、乱数復元、逆変換、OAEP+逆変換などの必要なプログラムを実行することで、送受信部24で受信した暗号文を平文に復号する。なお、メモリ23には、公開情報や秘密鍵などの復号化に必要な情報が格納されている。

[0046] 1. 第1実施形態

図3は、本発明の第1実施形態による暗号化／復号化装置の機能的構成を示すブ

ロック図である。本実施形態による暗号化／復号化装置は、平文を暗号化するための暗号化装置100と、暗号文を平文に復号するための復号化装置200とを有し、さらに鍵生成装置300により生成された暗号化／復号化に必要な公開情報を記憶する公開情報記憶装置301、復号化に必要な秘密鍵情報を記憶する秘密鍵記憶装置302を有する。

- [0047] 平文は、平文入力装置101により暗号化装置100へ与えられ、暗号化装置100にはOAEP+変換部102、変換関数Aによる変換部103およびNTRU暗号化部104などのプロセスが実現されている。暗号化装置100により生成された暗号文は暗号文出力装置105を通して、例えば受信端末へ出力される。
- [0048] 暗号文は、暗号文入力装置201により復号化装置200へ与えられ、復号化装置200にはNTRU復号化部202、乱数復元部203、変換関数Aの逆変換部204、OAEP+逆変換部205などのプロセスが実現されている。復号化装置200により生成された平文は平文出力装置206を通して出力される。
- [0049] 1. 1) 鍵生成
まず鍵生成手順を説明する。
- [0050] 図4は、第1実施形態における鍵生成手順を示すフローチャートである。鍵生成装置300は、正整数 p, q, N をとり、領域変数として公開する。上述したNTRU暗号方式と同様に、 $R = \mathbb{Z}[X]/(X^N - 1)$ とし、 R の元 u であって u の各次数の係数のうち a 個が1で b 個が-1、他のものが0であるもの全体の集合(R の部分集合)を $L(a, b)$ で表すものとし、 R の部分集合 L_f, L_g, L_r, L_m を取る(ステップS11)。
- [0051] さらに鍵生成装置1は、OAEP+パディング方式で説明したように、パラメータ k, k_0, k_1 を次のように選ぶ: k, k_0, k_1 は正整数、かつ、 $k_0 + k_1 \leq k \leq L$ を満たす。ここで、 L は $L_m \times L_r$ の元の数である。さらに、 $n = k - k_0 - k_1$ とし、
 G は、 k ビットのビット列に n ビットのビット列を対応させるハッシュ関数、
 H' は、 $n+k_0$ ビットのビット列に k_1 ビットのビット列を対応させるハッシュ関数、および、
 H は、 $n+k_1$ ビットのビット列に k_0 ビットのビット列を対応させるハッシュ関数とする(ステップS12)。
- [0052] さらに、鍵生成装置1は変換関数Aを決定する(ステップS13)。変換関数Aは k ビッ

ト以下のビット列に $L_m \times L_r$ の元を対応させる写像とし、以下の性質を満たさねばならない。

- [0053] (1) Aは単射であること
 (2) Aおよびその逆写像が多項式時間で計算できること
 (3) 暗号化関数を $E(m, r)$ とした時、写像 $E: A(X) \rightarrow L_e$ は、一方向性関数であること(ただし、Xは(m, r)の取りうる範囲を表し、 L_e は暗号文全体の空間を表す)。
- [0054] 鍵生成装置1は、NTRUと同様の方法で鍵生成を実行する。すなわち L_f から f を、 L_g から g をランダムに取り、 $h = f^{-1}g \bmod q$ とする。 f, g を秘密鍵とし、 h を公開鍵とする(ステップS14)。鍵生成装置1は、 f, g を秘密鍵記憶装置302に秘密裡に保持し(ステップS15)、NTRUの公開鍵、上記ハッシュ関数および変換関数($p, q, N, L_f, L_g, L_r, L_m, k, k_0, k_1, G, H', H, A, h$)を公開情報記憶装置301に格納して公開する(ステップS16)。
- [0055] 1. 2) 暗号化手順
 次に暗号化手順を説明する。
- [0056] 図5は、第1実施形態における暗号化手順を示すフローチャートである。暗号化装置100は、まず平文入力装置101から n ビットの平文 M を受け取り(ステップS21)、公開情報記憶装置301から公開情報 $p, q, N, L_f, L_g, L_r, L_m, k, k_0, k_1, G, H', H, A$ 、および h を受け取る(ステップS22)。
- [0057] 続いて、 k_0 ビットのビット列 R をランダムに選び(ステップS23)、OAEP+変換部102は、 $G(R)$ と M のビット毎の排他的論理和 s^0 を計算し、 $s^1 = H'(R||M)$ を計算し、 $s = s^0 || s^1$ とし、さらに、 $t = H(s)$ と R のビット毎の排他的論理和として、 $w = s || t$ を生成することで、平文をOAEP+パディングする(ステップS24)。
- [0058] さらに、変換部103は変換関数 A を用いて、 $(m, r) = A(w)$ によって、 w を2つのビット列 m および r に変換する(ステップS25)。ここでは、 w を等分割して前半のビット列を m 、後半のビット列を r とする。そして、NTRU暗号化部104は、 $e = phr + m \bmod q$ を計算することでNTRU暗号化を行い(ステップS26)、生成された暗号文を暗号文出力装置105から出力する(ステップS27)。
- [0059] 1. 3) 復号化手順

最後に復号化手順を説明する。

- [0060] 図6は、第1実施形態における復号化手順を示すフローチャートである。まず復号化装置200は暗号文入力装置201から暗号文 e を受け取り(ステップS31)、続いて、秘密鍵記憶装置302から暗号文に対応する秘密鍵を、公開情報記憶装置301からその秘密鍵に対応する公開情報を受け取る(ステップS32)。
- [0061] NTRU復号部202は、公開情報および秘密鍵を用いて、NTRU暗号方式と同様に暗号文 e の復号化処理を行う。すなわち、 $fe = pgr + fm \bmod q$ を計算し、 f, g, r, m がそれぞれ L_f, L_g, L_r, L_m の元であることから $fe = pgr + fm$ であるので、 $fe \bmod p = m \bmod p$ を計算することができ、 m が L_m の元であることから $m = m \bmod p$ なので、 m を復元できる(ステップS33)。
- [0062] また、乱数復元部203は、 $fe = pgr + fm$ であるので、 $r = (fe - fm)/pg$ により r を復元する(ステップS34)。
- [0063] 次に、逆変換部204は変換関数 A の逆変換を用いて、 $A^{-1}(m, r)$ により、 $w = s \| t = s_0 \| s_1 \| t$ を復元する(ステップS35)。続いて、OAEP+逆変換部205は、 $H(s)$ と t のビット毎の排他的論理和を取ることににより R を復元し、 $G(R)$ と s_0 のビット毎の排他的論理和を計算することにより M を復元する(ステップS36)。
- [0064] 最後に、パディングが正当であるか否かを $s_1 = H'(R \| M)$ が満たされるか否かによって判断し(ステップS37)、正当であれば平文 M を出力し(ステップS38)、正当でなければ暗号文 e は不正な暗号文として \perp を出力する(ステップS39)。
- [0065] 2. 第2実施形態
- 図7は、本発明の第2実施形態による暗号化／復号化装置の機能的構成を示すブロック図である。本実施形態による暗号化／復号化装置は、平文を暗号化するための暗号化装置400と、暗号文を平文に復号するための復号化装置500とを有し、さらに鍵生成装置300により生成された暗号化／復号化に必要な公開情報を記憶する公開情報記憶装置301、復号化に必要な秘密鍵情報を記憶する秘密鍵記憶装置302を有する。
- [0066] 平文は、平文入力装置101により暗号化装置400へ与えられ、暗号化装置400には乱数発生部401、秘密鍵暗号化部402、OAEP+変換部403、変換関数 A による変

換部404およびNTRU暗号化部405などのプロセスが実現されている。暗号化装置400により生成された暗号文は暗号文出力装置105を通して、例えば受信端末へ出力される。

[0067] 暗号文は、暗号文入力装置201により復号化装置500へ与えられ、復号化装置500にはNTRU復号化部501、乱数復元部502、変換関数Aの逆変換部503、OAEP+逆変換部504、秘密鍵暗号復号部505などのプロセスが実現されている。復号化装置500により生成された平文は平文出力装置206を通して出力される。

[0068] 2. 1)鍵生成

まず鍵生成手順を説明する。

[0069] 図8は、第2実施形態における鍵生成手順を示すフローチャートである。鍵生成装置300は、正整数 p, q, N をとり、領域変数として公開する。上述したNTRU暗号方式と同様に、 $R = \mathbb{Z}[X]/(X^N - 1)$ とし、 R の元 u であって u の各次数の係数のうち a 個が1で b 個が-1、他のものが0であるもの全体の集合(R の部分集合)を $L(a, b)$ で表すものとし、 R の部分集合 L_f, L_g, L_r, L_m を取る(ステップS41)。

[0070] さらに鍵生成装置1は、OAEP+パディング方式で説明したように、パラメータ k, k_0, k_1 を次のように選ぶ: k, k_0, k_1 は正整数、かつ、 $k_0 + k_1 \leq k \leq L$ を満たす。ここで、 L は $L_m \times L_r$ の元の数である。さらに、 $n = k - k_0 - k_1$ とし、
 G は、 k ビットのビット列に n ビットのビット列を対応させるハッシュ関数、
 H' は、 $n+k_0$ ビットのビット列に k_1 ビットのビット列を対応させるハッシュ関数、および、
 H は、 $n+k_1$ ビットのビット列に k_0 ビットのビット列を対応させるハッシュ関数とする(ステップS42)。

[0071] さらに、鍵生成装置1は変換関数 A を決定する(ステップS43)。変換関数 A は、上述したように、 k ビット以下のビット列に $L_m \times L_r$ の元を対応させる写像とし、以下の性質を満たさねばならない。

[0072] (1) A は単射であること

(2) A およびその逆写像が多項式時間で計算できること

(3)暗号化関数を $E(m, r)$ とした時、写像 $E: A(X) \rightarrow L_e$ は、一方向性関数であること(ただし、 X は (m, r) の取りうる範囲を表し、 L_e は暗号文全体の空間を表す)。

- [0073] 鍵生成装置1は、NTRUと同様の方法で鍵生成を実行する。すなわち L_f から f を、 L_g から g をランダムに取り、 $h = f^{-1}g \bmod q$ とする。 f 、 g を秘密鍵とし、 h を公開鍵とする。鍵生成装置1は、 f 、 g を秘密鍵記憶装置302に秘密裡に保持し(ステップS44)する。
- [0074] さらに、鍵生成装置1は、使用する共通鍵暗号方式Eを決定し(ステップS45)、NTRUの公開鍵、上記ハッシュ関数および変換関数(p , q , N , L_f , L_g , L_r , L_m , k , k_0 , k_1 , G , H' , H , A , h)を公開情報記憶装置301に格納して公開する(ステップS46)。
- [0075] 2. 2)暗号化手順
次に暗号化手順を説明する。
- [0076] 図9は、第2実施形態における暗号化手順を示すフローチャートである。暗号化装置400は、まず平文入力装置101から n ビットの平文 X を受け取り(ステップS51)、公開情報記憶装置301から公開情報 p , q , N , L_f , L_g , L_r , L_m , k , k_0 , k_1 , G , H' , H , A , および h を受け取る(ステップS52)。
- [0077] 続いて、乱数発生部401を用いて秘密鍵暗号化部402は n ビットのビット列 M をランダムに選び(ステップS53)、 $Y = E_M(X)$ を計算して共通鍵暗号化を行う(ステップS54)。ここで、 $E_M(X)$ は、 M を鍵として平文 X を共通鍵暗号方式Eに従って暗号化したものである。
- [0078] 続いて、 k_0 ビットのビット列 R をランダムに選び(ステップS55)、OAEP+変換部403は、 $G(R)$ と M のビット毎の排他的論理和 s^0 を計算し、 $s^1 = H'(R||M)$ を計算し、 $s = s^0 || s^1$ とし、さらに、 $t = H(s)$ と R のビット毎の排他的論理和として、 $w = s || t$ を生成することで、平文をOAEP+パディングする(ステップS56)。
- [0079] さらに、変換関数Aによる変換部404は、 $(m, r) = A(w)$ によって w を2つのビット列 m および r に変換する(ステップS57)。ここでは、 w を2分割して前半のビット列を m 、後半のビット列を r とする。そして、NTRU暗号化部405は、 $e = phr + m \bmod q$ を計算することでNTRU暗号化を行い(ステップS58)、生成された暗号文 e と共通鍵暗号の暗号文 Y とを暗号文 (e, Y) として暗号文出力装置105から出力する(ステップS59)。
- [0080] 2. 3)復号化手順
最後に復号化手順を説明する。
- [0081] 図10は、第2実施形態における復号化手順を示すフローチャートである。まず復号

化装置500は暗号文入力装置201から暗号文eを受け取り(ステップS61)、続いて、秘密鍵記憶装置302から暗号文に対応する秘密鍵を、公開情報記憶装置301からその秘密鍵に対応する公開情報を受け取る(ステップS62)。

[0082] NTRU復号化部501は、公開情報および秘密鍵を用いて、NTRU暗号方式と同様に暗号文eの復号化処理を行う。すなわち、 $fe = pgr + fm \bmod q$ を計算し、 f, g, r, m がそれぞれ L_f, L_g, L_r, L_m の元であることから $fe = pgr + fm$ であるので、 $fe \bmod p = m \bmod p$ を計算することができ、 m が L_m の元であることから $m = m \bmod p$ なので、 m を復元できる(ステップS63)。

[0083] また、乱数復元部502は、 $fe = pgr + fm$ であるので、 $r = (fe - fm)/pg$ により r を復元する(ステップS64)。

[0084] 次に、逆変換部503は、 $A^{-1}(m, r)$ により、 $w = s_0 || t = s_0 || s_1 || t$ を復元する(ステップS65)。続いて、OAEP+逆変換部504は、 $H(s)$ と t のビット毎の排他的論理和を取ることにより R を復元し、 $G(R)$ と s_0 のビット毎の排他的論理和を計算することにより M を復元する(ステップS66)。

[0085] 最後に、パディングが正当であるか否かを $s_1 = H'(R || M)$ が満たされるか否かによって判断し(ステップS67)、正当であれば、共通鍵暗号の鍵 M を用いて共通鍵暗号を解き、平文 X を出力し(ステップS68)、正当でなければ暗号文 e は不正な暗号文として \perp を出力する(ステップS69)。

図面の簡単な説明

[0086] [図1](A)は、本発明によるパディング適用方式による暗号化装置の概念的ブロック図であり、(B)は従来例によるOAEPベースのパディング方式を適用した暗号化装置の概念的ブロック図である。

[図2]本発明による暗号化／復号化装置を実装した暗号通信システムの一例を示すブロック図である。

[図3]本発明の第1実施形態による暗号化／復号化装置の機能的構成を示すブロック図である。

[図4]第1実施形態における鍵生成手順を示すフローチャートである。

[図5]第1実施形態における暗号化手順を示すフローチャートである。

[図6]第1実施形態における復号化手順を示すフローチャートである。

[図7]本発明の第2実施形態による暗号化／復号化装置の機能的構成を示すブロック図である。

[図8]第2実施形態における鍵生成手順を示すフローチャートである。

[図9]第2実施形態における暗号化手順を示すフローチャートである。

[図10]第2実施形態における復号化手順を示すフローチャートである。

符号の説明

- [0087] 100 暗号化装置
- 101 平文入力装置
- 102 OAEP+変換部
- 103 変換関数Aによる変換部
- 104 NTRU暗号化部
- 105 暗号文出力装置
- 200 復号化装置
- 201 暗号文入力装置
- 202 NTRU復号化部
- 203 乱数復元部
- 204 変換関数Aの逆変換部
- 205 OAEP+逆変換部
- 206 平文出力装置
- 300 鍵生成装置
- 301 公開情報記憶装置
- 302 秘密鍵記憶装置

請求の範囲

- [1] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用する方法において、
- 入力情報を前記パディング方式により所定長以下のビット列に変換し、
- 前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換し、
- 前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給し、
- 前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、
- ことを特徴とするパディング適用方法。
- [2] 前記変換規則は、前記ビット列の前半を前記第1ビット列とし、後半を前記第2ビット列とするように前記ビット列を2分割する規則であることを特徴とする請求項1に記載のパディング適用方法。
- [3] 前記パディング方式はOAEP+パディングであり、前記乱数を使用する暗号化方式はNTRU暗号方式であることを特徴とする請求項1または2に記載のパディング適用方法。
- [4] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用する方法において、
- 入力情報を前記パディング方式により所定長以下のビット列に変換するパディング変換手段と、
- 前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換するビット列変換手段と、
- 前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して暗号文を生成する暗号化手段と、

前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、ことを特徴とするパディング装置。

- [5] 前記変換規則は、前記ビット列の前半を前記第1ビット列とし、後半を前記第2ビット列とするように前記ビット列を2分割する規則であることを特徴とする請求項4に記載のパディング装置。

- [6] 前記パディング方式はOAEP+パディングであり、前記乱数を使用する暗号化方式はNTRU暗号方式であることを特徴とする請求項4または5に記載のパディング装置。

- [7] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用することで暗号文を生成する暗号化装置において、

入力した平文を前記パディング方式により所定長以下のビット列に変換するパディング変換手段と、

前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換するビット列変換手段と、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して暗号文を生成する暗号化手段と、

前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、

ことを特徴とする暗号化装置。

- [8] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用することで暗号文を生成する暗号化装置において、

秘密鍵暗号の鍵をランダムに選択し、前記秘密鍵暗号の鍵を用いて、入力した平文を秘密鍵暗号化することで第1暗号文を生成する第1暗号化手段と、

前記秘密鍵暗号の鍵を前記パディング方式により所定長以下のビット列に変換するパディング変換手段と、

前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換するビット列変換手段と、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して第2暗号文を生成する第2暗号化手段と、

前記第1暗号文および前記第2暗号文を暗号文として出力する暗号文出力手段と

、
を有し、前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、
ことを特徴とする暗号化装置。

[9] 前記変換規則は、前記ビット列の前半を前記第1ビット列とし、後半を前記第2ビット列とするように前記ビット列を2分割する規則であることを特徴とする請求項7または8に記載の暗号化装置。

[10] 前記パディング方式はOAEP+パディングであり、前記乱数を使用する暗号化方式はNTRU暗号方式であることを特徴とする請求項7または8に記載の暗号化装置。

[11] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用することで暗号文を生成する方法において、

入力した平文を前記パディング方式により所定長以下のビット列に変換し、

前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換し、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して暗号文を生成し、

前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、
ことを特徴とする暗号化方法。

- [12] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用することで暗号文を生成する方法において、

秘密鍵暗号の鍵をランダムに選択し、

前記秘密鍵暗号の鍵を用いて、入力した平文を秘密鍵暗号化することで第1暗号文を生成し、

前記秘密鍵暗号の鍵を前記パディング方式により所定長以下のビット列に変換し、

前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換し、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して第2暗号文を生成し、

前記第1暗号文および前記第2暗号文を暗号文として出力し、

前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、
ことを特徴とする暗号化方法。

- [13] 前記変換規則は、前記ビット列の前半を前記第1ビット列とし、後半を前記第2ビット列とするように前記ビット列を2分割する規則であることを特徴とする請求項11または12に記載の暗号化方法。

- [14] 前記パディング方式はOAEP+パディングであり、前記乱数を使用する暗号化方式はNTRU暗号方式であることを特徴とする請求項11または12に記載の暗号化方法。

- [15] 請求項7に記載の暗号化装置により生成された暗号文を復号化する装置において

、
前記乱数を使用する暗号化方式に対応する復号化方式に従って、入力した暗号文を復号化して第1ビット列を生成する第1復号化手段と、
前記暗号化に使用した乱数を第2ビット列として復元する乱数復号手段と、
前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を所定長以下のビット列に逆変換するビット列逆変換手段と、
前記所定長以下のビット列から前記パディング方式によるパディングを除去することで元の平文を生成するパディング逆変換手段と、
前記パディングの正当性を判断し、正当であれば前記平文を出力する判定手段と
、
を有することを特徴とする復号化装置。

[16] 請求項8に記載の暗号化装置により生成された暗号文を復号化する装置において

、
前記乱数を使用する暗号化方式に対応する復号化方式に従って、前記第2暗号文を復号化して第1ビット列を生成する第1復号化手段と、
前記暗号化に使用した乱数を第2ビット列として復元する乱数復号手段と、
前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を所定長以下のビット列に逆変換するビット列逆変換手段と、
前記所定長以下のビット列から前記パディング方式によるパディングを除去することで元の秘密鍵暗号の鍵を生成するパディング逆変換手段と、
前記パディングの正当性を判断し、正当であれば前記秘密鍵暗号の鍵を用いて前記第1暗号文を復号する第2復号手段と、
を有することを特徴とする復号化装置。

[17] 請求項11に記載の暗号化方法により生成された暗号文を復号化する方法において、

前記乱数を使用する暗号化方式に対応する復号化方式に従って、入力した暗号文を復号化して第1ビット列を生成し、
前記暗号化に使用した乱数を第2ビット列として復元し、

前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を
所定長以下のビット列に逆変換し、

前記所定長以下のビット列から前記パディング方式によるパディングを除去すること
で元の平文を生成し、

前記パディングの正当性を判断し、正当であれば前記平文を出力する、
ことを特徴とする復号化方法。

- [18] 請求項12に記載の暗号化方法により生成された暗号文を復号化する方法において、

前記乱数を使用する暗号化方式に対応する復号化方式に従って、前記第2暗号
文を復号化して第1ビット列を生成し、

前記暗号化に使用した乱数を第2ビット列として復元し、

前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を
所定長以下のビット列に逆変換し、

前記所定長以下のビット列から前記パディング方式によるパディングを除去すること
で元の秘密鍵暗号の鍵を生成し、

前記パディングの正当性を判断し、正当であれば前記秘密鍵暗号の鍵を用いて前
記第1暗号文を復号する、

ことを特徴とする復号化方法。

- [19] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方
式と、乱数を使用しない暗号化方式で安全性が保証されたパディング方式とを用い、
通信ネットワークを通して通信端末間で暗号通信を行うシステムにおいて、

送信側通信端末は、

入力した平文を前記パディング方式により所定長以下のビット列に変換するパデ
ィング変換手段と、

前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直
積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像および
その逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする
前記暗号化関数が一方向性関数であること、を満たす変換規則に従って、前記ビッ

ト列を第1ビット列と第2ビット列とに変換するビット列変換手段と、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して暗号文を生成する暗号化手段と、

前記暗号文を受信側端末へ送信する送信手段と、

を有し、

前記受信側通信端末は、

前記暗号文を前記送信側通信端末から受信する受信手段と、

前記乱数を使用する暗号化方式に対応する復号化方式に従って、入力した暗号文を復号化して第1ビット列を生成する第1復号化手段と、

前記暗号化に使用した乱数を第2ビット列として復元する乱数復号手段と、

前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を所定長以下のビット列に逆変換するビット列逆変換手段と、

前記所定長以下のビット列から前記パディング方式によるパディングを除去することで元の平文を生成するパディング逆変換手段と、

前記パディングの正当性を判断し、正当であれば前記平文を出力する判定手段と、

を有する、

ことを特徴とする暗号通信システム。

[20] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式と、乱数を使用しない暗号化方式で安全性が保証されたパディング方式とを用い、通信ネットワークを通して通信端末間で暗号通信を行うシステムにおいて、

送信側通信端末は、

秘密鍵暗号の鍵をランダムに選択し、前記秘密鍵暗号の鍵を用いて、入力した平文を秘密鍵暗号化することで第1暗号文を生成する第1暗号化手段と、

前記秘密鍵暗号の鍵を前記パディング方式により所定長以下のビット列に変換するパディング変換手段と、

前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像および

その逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす変換規則に従って、前記ビット列を第1ビット列と第2ビット列とに変換するビット列変換手段と、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して第2暗号文を生成する第2暗号化手段と、

前記第1暗号文および前記第2暗号文を暗号文として出力する暗号文出力手段と、

を有し、

前記受信側通信端末は、

前記暗号文を前記送信側通信端末から受信する受信手段と、

前記乱数を使用する暗号化方式に対応する復号化方式に従って、前記第2暗号文を復号化して第1ビット列を生成する第1復号化手段と、

前記暗号化に使用した乱数を第2ビット列として復元する乱数復号手段と、

前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を所定長以下のビット列に逆変換するビット列逆変換手段と、

前記所定長以下のビット列から前記パディング方式によるパディングを除去することで元の秘密鍵暗号の鍵を生成するパディング逆変換手段と、

前記パディングの正当性を判断し、正当であれば前記秘密鍵暗号の鍵を用いて前記第1暗号文を復号する第2復号手段と、

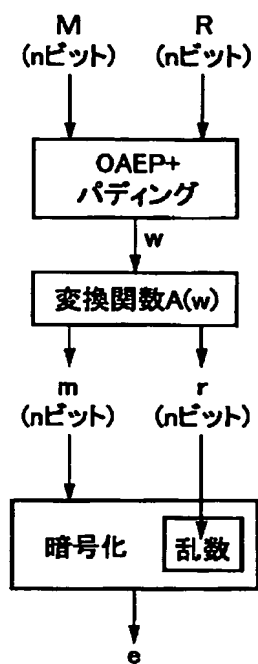
を有する、

ことを特徴とする暗号通信システム。

[図1]

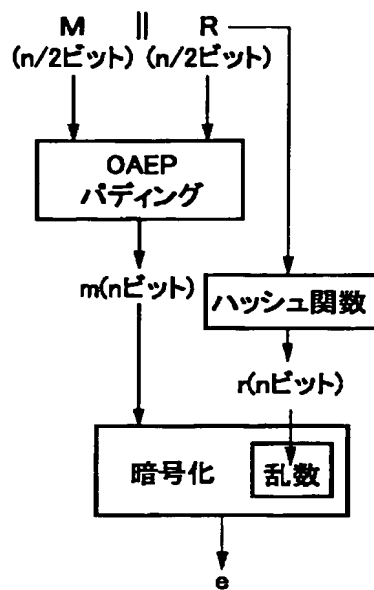
(A)

(本発明)

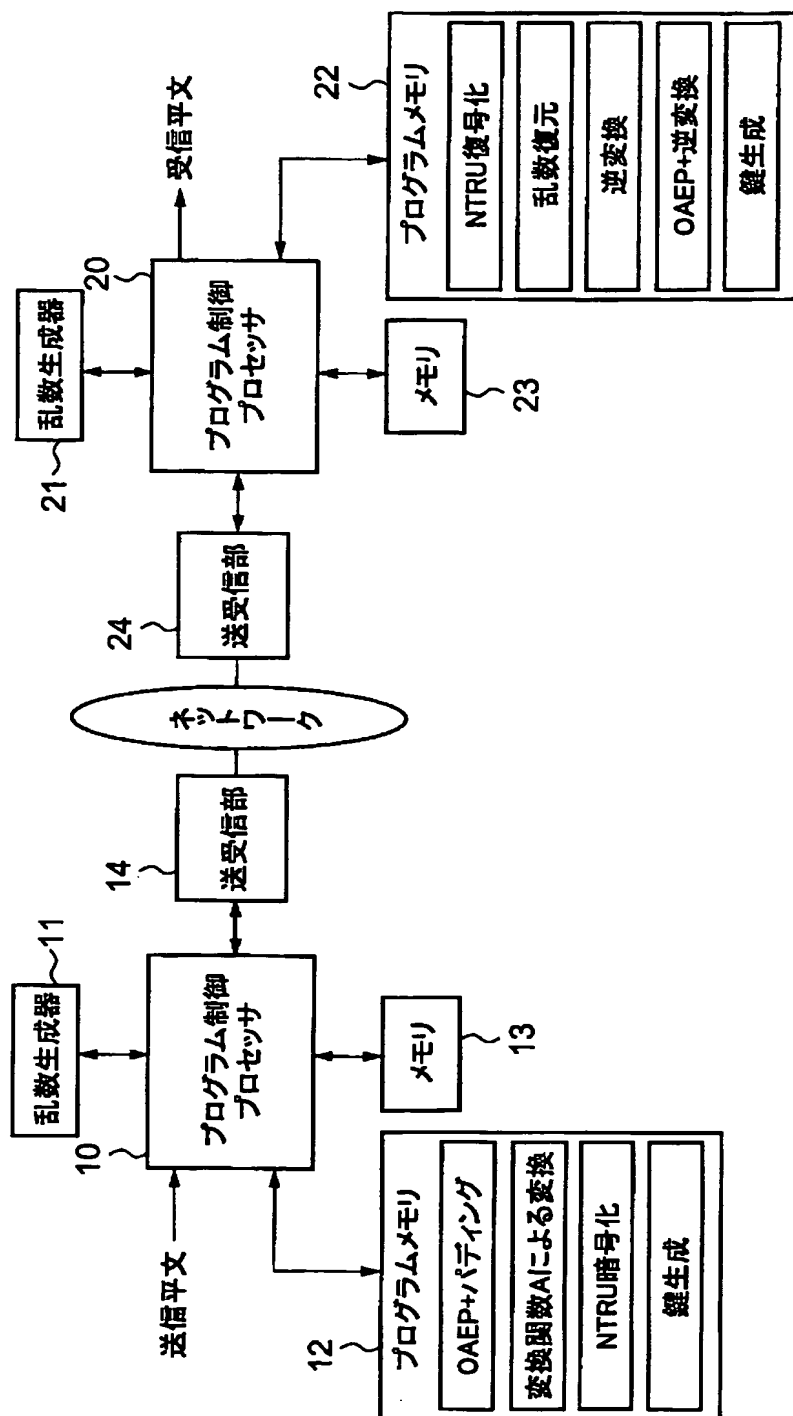


(B)

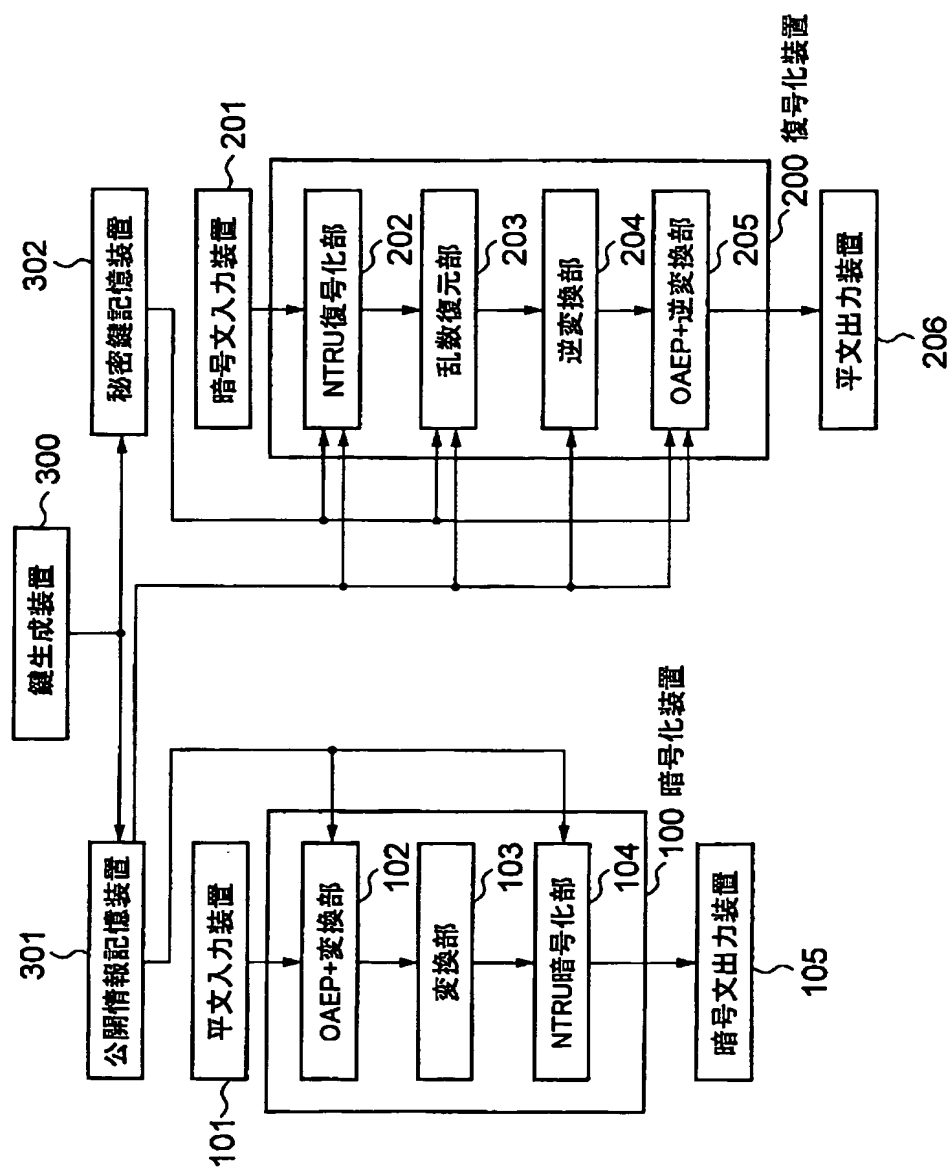
(従来例)



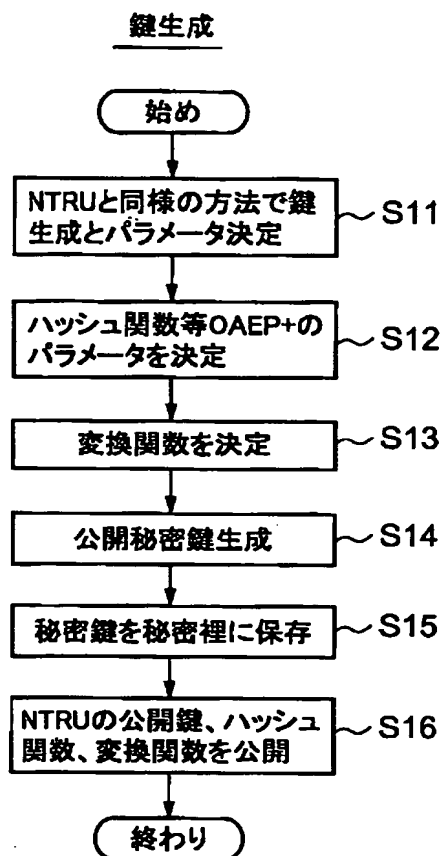
[図2]



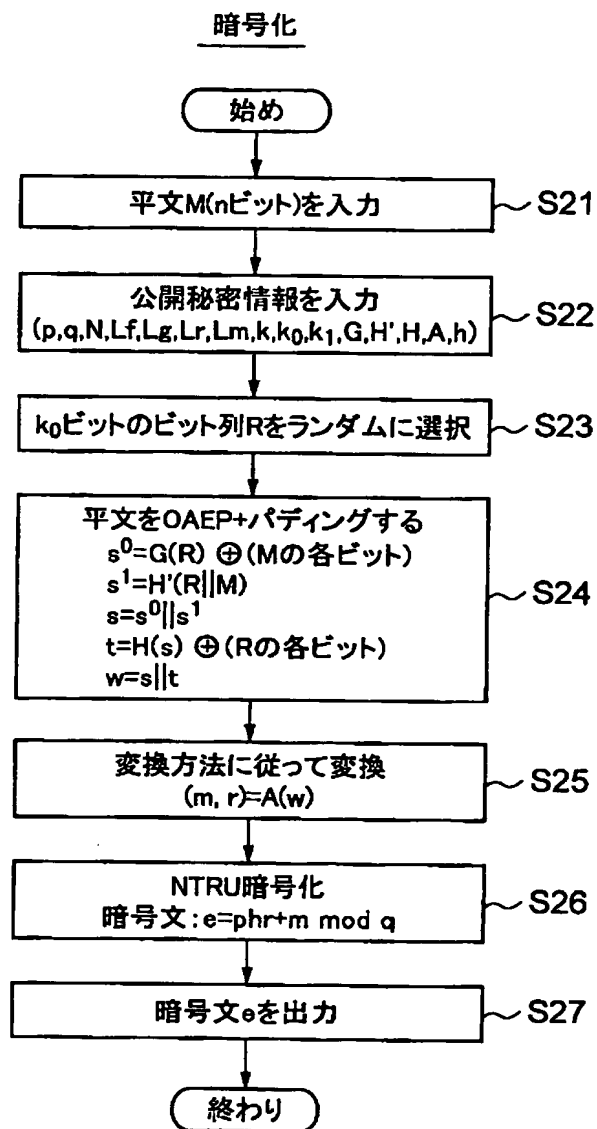
[図3]



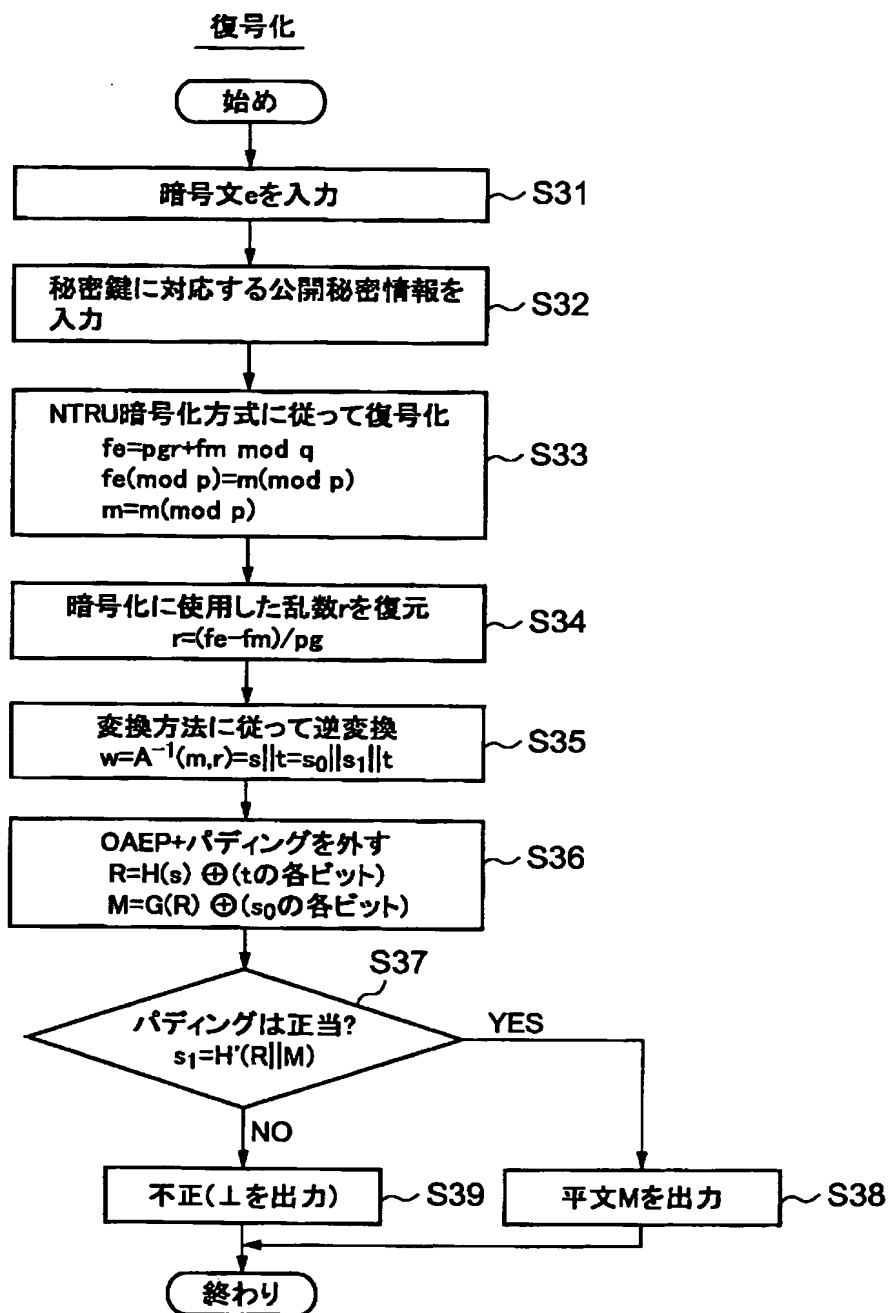
[図4]



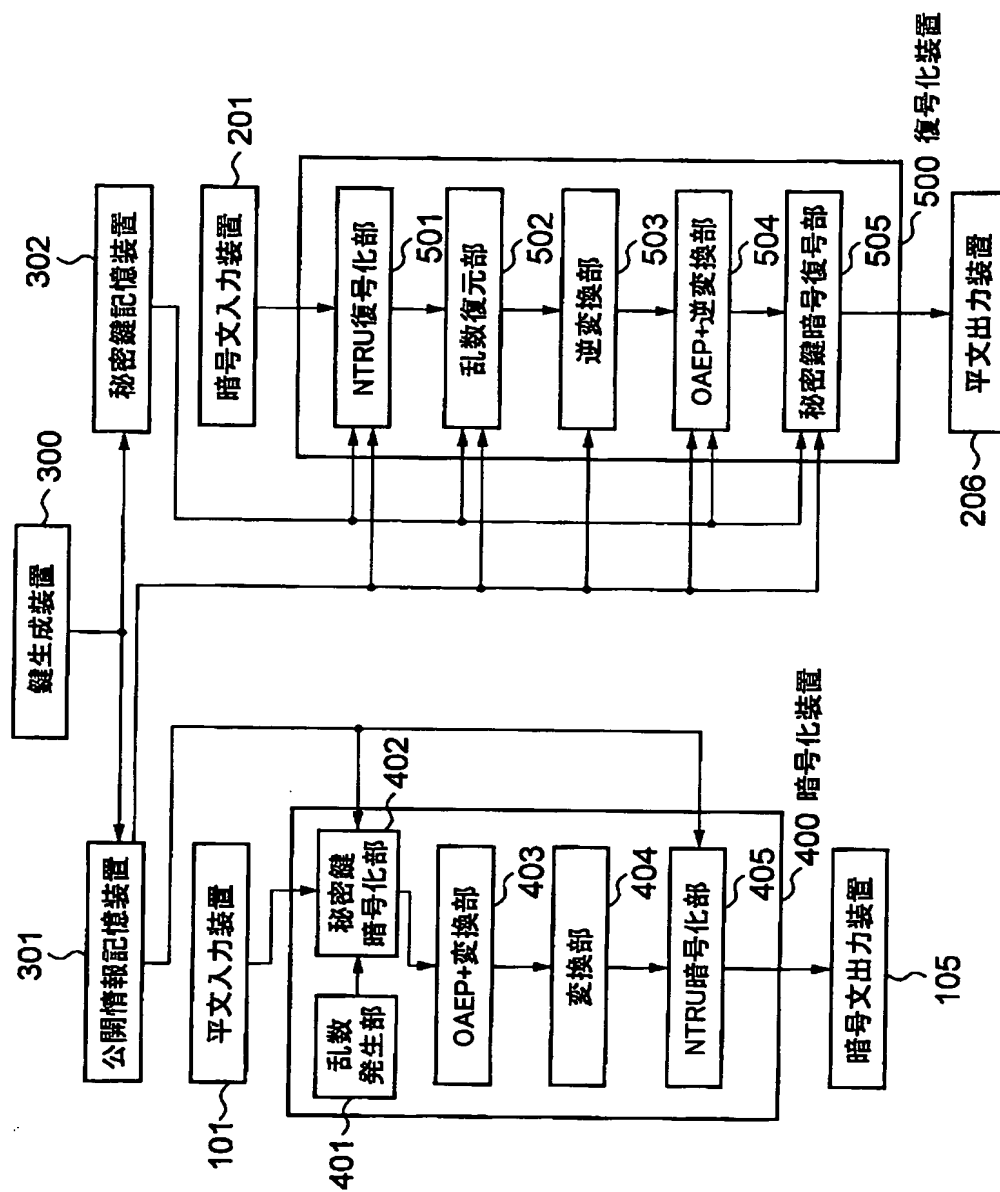
[図5]



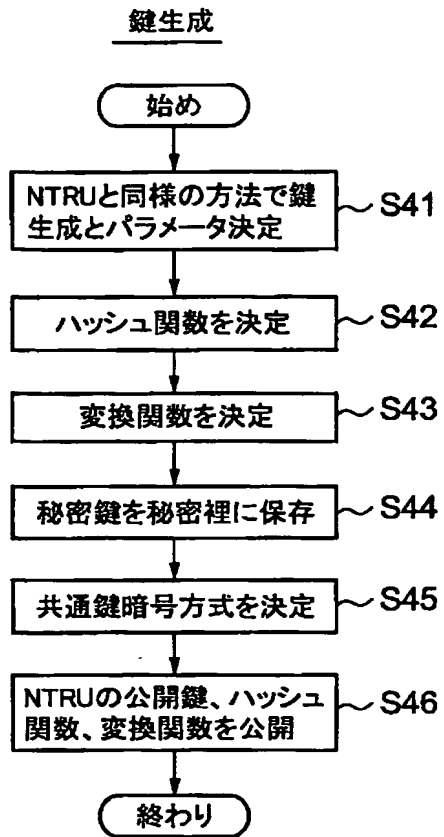
[図6]



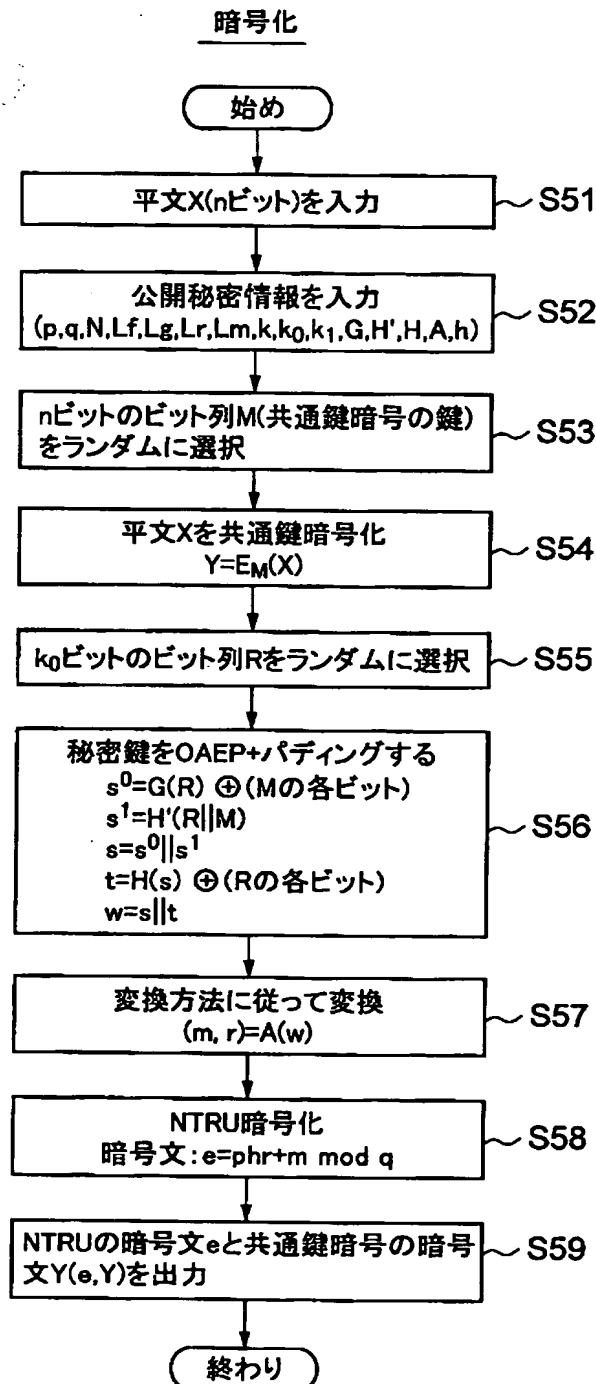
[図7]



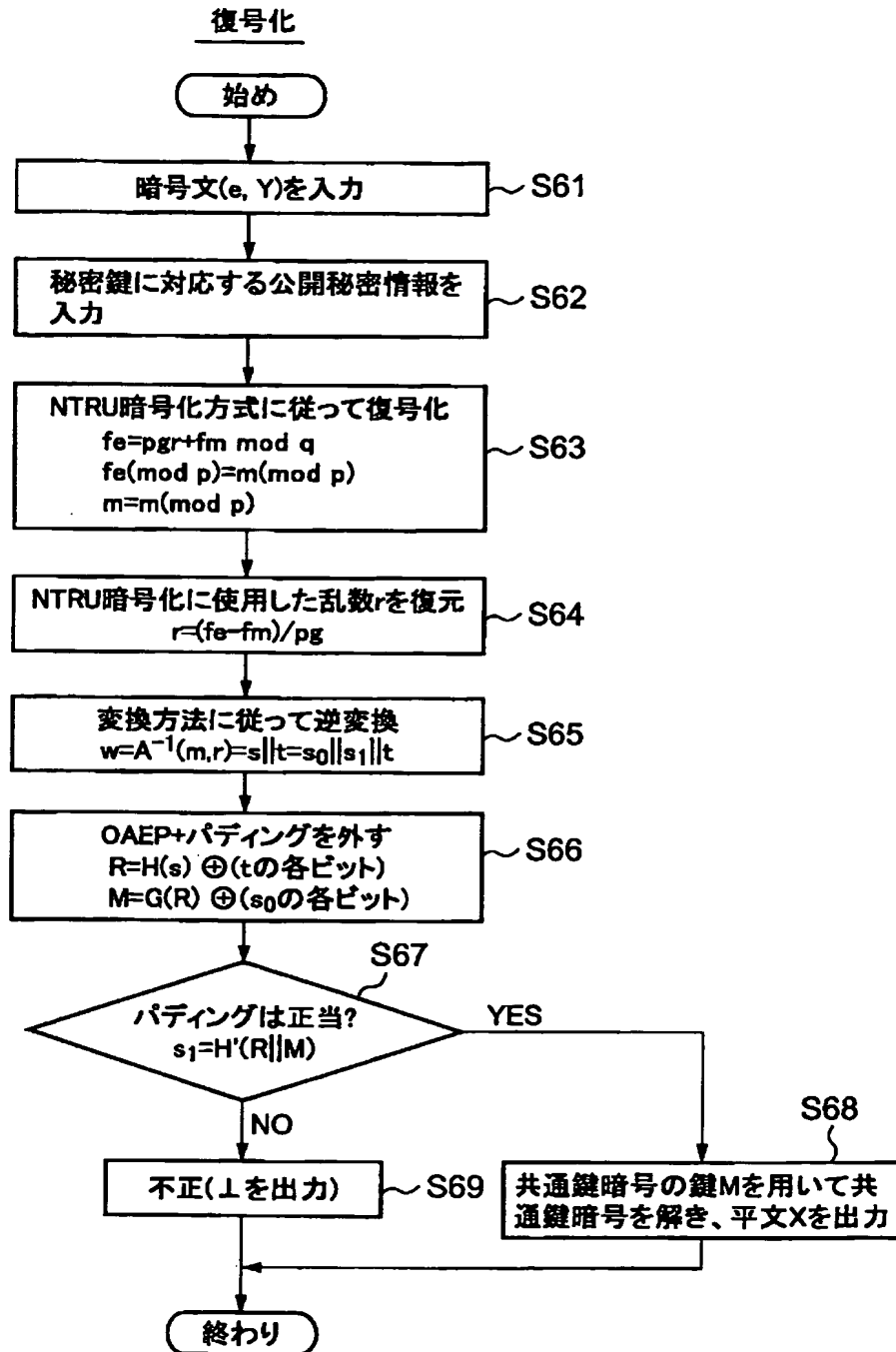
[図8]



[図9]



[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/005287

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G09C1/00Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus FILE (JOIS), NTRU, OAEP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SHOUP V., OAEP Reconsidered (Extended Abstract), LNCS, Vol.2139, 2001, pages 239 to 259	1-20
A	NGUYEN P.Q., POINTCHEVAL D., Analysis and Improvements of NTRU Encryption Paddings, LNCS, Vol.2442, 2002, pages 210 to 225	1-20
A	JP 2000-516733 A (NTRU Cryptosystems, Inc.), 12 December, 2000 (12.12.00), Full text & US 6081597 A & EP 920753 A & WO 1998/8323 A1 & AU 4582897 A & CA 2263588 A & CN 1232588 A	1-20

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
20 April, 2005 (20.04.05)Date of mailing of the international search report
17 May, 2005 (17.05.05)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl.⁷ G09C1/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl.⁷ G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2005年
日本国実用新案登録公報	1996-2005年
日本国登録実用新案公報	1994-2005年

国際調査で利用した電子データベース (データベースの名称、調査に使用した用語)

JSTPlusファイル(JOIS), NTRU, OAEP

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	SHOUP V, OAEP Reconsidered (Extended Abstract), LNCS, Vol. 2139, 2001, p. 239-259	1-20
A	NGUYEN P Q, POINTCHEVAL D, Analysis and Improvements of NTRU Encryption Paddings, LNCS, Vol. 2442, 2002, p. 210-225	1-20

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

20.04.2005

国際調査報告の発送日

17.05.2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石田 信行

電話番号 03-3581-1101 内線 3599

5M 3365

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2000-516733 A (エヌティーアールユー クリプトシステムズ, インコーポレーテッド) 2000. 12. 12, 全文 & US 6081597 A & EP 920753 A & WO 1998/8323 A1 & AU 4582897 A & CA 2263588 A & CN 1232588 A	1-20